**13:69E-1.26A Bill changers with electrically erasable/programmable storage media**

(a) All program code for bill changers with electrically erasable/programmable storage media shall:

1. Be capable of detecting 99.99 percent of all possible failures or changes in the bill changer program;

2. Utilize a Cyclic Redundancy Check, or other method approved by the Division:

i. Yield, at a minimum, a four-digit hex number; and

ii. Be included in the bill changer software, including any upgrade;

3. Be subject to testing utilizing at least two confidential seed inputs provided by the manufacturer to the Division, the results of which testing shall:

i. Be read on a portable computer or other device approved by the Division; and

ii. Require the bill changer to be placed in a hard tilt state when either seed fails to yield the predicted result, regardless whether such failure occurs at installation or at anytime thereafter;

4. Provide verification that the bill changer code has not been altered via the cyclic redundancy check required in (a)2 above, which verification shall occur:

i. In a manner tested and approved by the Division; and

ii. At a minimum, whenever power is restored to the slot machine and after any software download to the bill changer.

**13:69E-1.26B Gaming equipment and related devices utilizing alterable storage media**

(a) "Alterable storage media" shall mean a memory chip or other storage medium, such as a FLASH chip, CD-ROM or hard disk, which is contained in a slot machine, or other gaming equipment or related device subject to testing and approval by the Division, but does not include a printer, display, bill changer or other peripheral device which does not affect the outcome of a game. Alterable storage media may include media that are:

1. Erasable or reprogrammable without being removed from the gaming equipment or related device, such as an EPROM or hard disk; or

2. Removable and replaceable, such as a CD-ROM or a diskette.

(b) Each manufacturer of gaming equipment and related devices pursuant to (a) above that utilizes alterable storage media, other than a bill validator, shall identify any data, files, and programs that may be written to alterable storage media and specify, at a minimum, the data type such as game state and meter information, the location to which the data shall be written, and the need for the written data.

(c) Except as otherwise permitted in (i) below, alterable storage media shall comply with the requirements of (d) through (h) below.

(d) Gaming equipment and related devices pursuant to (a) above that utilize alterable storage media shall only write to alterable storage media containing data, files, and programs that are not critical to the basic operation of a game, such as marketing information. Notwithstanding the foregoing, gaming equipment and related devices may write to alterable storage media containing critical data, files, and programs provided that the gaming equipment or device:

1. Maintains a record, known as an authorization list or digital signature, of all information that is added, deleted, and modified on the media, which satisfies the requirements of (e) below; and

2. Verifies the validity of all data, files, and programs which reside on the media against the authorization list or digital signature by means of an algorithm or other method which satisfies the requirements of (f) below and is approved by the Division.

(e) The authorization list or digital signature maintained pursuant to (d)1 above shall be encrypted using a cryptographic system approved by the Division. Notwithstanding the foregoing, an authorization list or digital signature that resides on read-only storage media which is inspected and physically sealed or otherwise secured shall not require encryption.

(f) The authentication algorithm or other method utilized pursuant to (d) above shall:

1. Reside in and execute from storage media in the gaming equipment or related device pursuant to (a) above, which shall be incapable of being altered while installed in the device, inspected and physically sealed or otherwise secured and:

i. Located in a separate read-only storage media, such as an EPROM; or

ii. Partitioned from all other data.

2. Except for sound files and other types of computer files that do not affect the integrity or outcome of the game, execute for all computer files each time the gaming equipment or related device pursuant to (a) above is powered up, and when files are loaded from the media; and

3. Prevent further play of the gaming equipment or related device pursuant to (a) above if unexpected data or structural inconsistencies are detected.

(g) In the event that a failed authentication occurs in a slot machine, the slot machine shall:

1. Immediately enter into a state in which the game is not playable;

2. Automatically generate an alert notification of the tilt to the surveillance department and the slot shift manager, or such manager's supervisor, or, if gaming equipment and related devices are not capable of such alert notification, cause an appropriate tower light state, and the recording of the details of the tilt to include, at a minimum, type of tilt, time, date, and slot machine event in a log; and

3. If the slot machine is connected to an approved computerized slot monitoring system, send a specific signal to the casino licensee's slot monitoring system indicating a tilt mode that shall be reviewed.

(h) Each casino licensee shall immediately notify Division of all failed authentications.

(i) Notwithstanding any other provision of these regulations, no casino shall be required to file a separate report in compliance with N.J.A.C. 13:69D1.42(r)(3) or to report as gross revenue the greater of either the actual money collected in a slot cash storage box or the amount recorded on the appropriate meters of a corresponding slot machine on account of the use of bill changers utilizing alterable media.